

Listing of Claims:

This listing of claims will replace all prior versions, and listings of claims in the application. No claims have been added, amended or canceled.

1. (Previously Presented) A method for providing access to resources, comprising the steps of:

acquiring user identification information from a first authentication system, said user identification information is associated with a request from a first user to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said first authentication system;

relying on said first authentication system for authenticating said first user;

using said user identification information to access an identity profile associated with said user identification information; and

performing, at said authorization system, authorization services for said request to access said first resource based on said identity profile associated with said user identification information;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

2. (Original) A method according to claim 1, wherein:

said step of acquiring user identification includes reading a user ID from an internal web server variable.

3. (Original) A method according to claim 2, further comprising the step of:

allowing a first user to access said first resource if said step of performing determines that said first user is authorized to access said first resource based on said identity profile, said first user is associated with said identity profile and said request.

4. (Previously Presented) A method according to claim 1, wherein relying on said first authentication system comprises the steps of:

receiving information about said request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.

5. (Original) A method according to claim 1, wherein:

said step of acquiring user identification includes acquiring a plurality of data items which can be used to identify a user.

6. (Original) A method according to claim 1, further comprising the step of:

acquiring one or more data items in addition to said user identification information, said step of performing authorization services uses said one or more data items to attempt to authorize access to said first resource in response to said request.

7. (Original) A method according to claim 1, wherein:

said authorization system is part of an access system that protects a plurality of resources, said plurality of resources includes said first resource, a second resource and a third resource;

said first resource uses said first authentication system for authentication services;

said second resource uses a second authentication system for authentication services, said second authentication system is separate from said access system; and

said third resource uses a third authentication system for authentication services, said third authentication system is separate from said access system.

8. (Original) A method according to claim 7, wherein:

said first authentication system is a default web server authentication system;

said second authentication system is an authentication plug-in; and

said third authentication system is a third party authentication system.

9. (Original) A method according to claim 1, wherein:
said authorization system is part of an access system that protects a plurality of resources, said access system provides use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.
10. (Original) A method according to claim 1, wherein:
said authorization system is part of an access system that protects a plurality of resources and does not have an application program interface.
11. (Original) A method according to claim 1, further comprising the steps of:
using said user identification information to create information for a cookie; and
causing said cookie to be transmitted for storage on a client associated with said request.
12. (Original) A method according to claim 11, further comprising the step of:
performing single sign-on services based on said cookie.
13. (Original) A method according to claim 11, further comprising the steps of:
receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and
using said cookie to authorize access to said second resource without authenticating.
14. (Original) A method according to claim 11, further comprising the steps of:
receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.

15. (Previously Presented) A method for providing access to resources, comprising the steps of:

acquiring a plurality of variables from a first authentication system, said step of acquiring is performed by an authorization system, said authorization system is separate from said first authentication system, said variables are associated with a first request from a first user to access a first resource;

relying on said first authentication system for authenticating said first user;

performing, at said authorization system, authorization services for said request to access said first resource based on said plurality of variables;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

16. (Previously Presented) A method according to claim 15, wherein relying on said first authentication system comprises the steps of:

receiving information from said first request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.

17. (Original) A method according to claim 15, wherein:

said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

18. (Original) A method according to claim 15, further comprising the steps of:
using said plurality of variables to create information for a cookie; and
causing said cookie to be transmitted for storage on a client associated with said request.
19. (Original) A method according to claim 18, further comprising the step of:
performing single sign-on services based on said cookie.
20. (Original) A method according to claim 18, further comprising the steps of:
receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and
using said cookie at said second server to authorize access to said second resource without authenticating.
21. (Previously Presented) A method for providing access to resources, comprising the steps of:
acquiring user identification information from an authentication system, said user identification information is associated with a request from a first user to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said authentication system;
relying on said authentication system for authenticating said first user;
using said user identification information to create information for a cookie;
causing said cookie to be transmitted for storage on a client associated with said request to access said first resource; and
performing, at said authorization system, authorization services for said request to access said first resource;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

22. (Original) A method according to claim 21, wherein:

said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

23. (Original) A method according to claim 21, further comprising the step of:
performing single sign-on services based on said cookie.

24. (Original) A method according to claim 21, further comprising the steps of:
receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and
using said cookie to authorize access to said second resource without authenticating.

25. (Original) A method according to claim 21, further comprising the steps of:
receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and
using said cookie at said second server to authorize access to said second resource without authenticating.

26. (Previously Presented) A method for providing access to resources, comprising the steps of:

receiving, at an access system, configuration information for a first resource, said access system provides for using of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said configuration information provides an indication to said access system to rely on a first external authentication system for said first resource;

receiving a first request from a first user for said first resource;
relying on said first external authentication system for authenticating said first user; and

performing, at said authorization system, authorization services for said first request;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

27. (Original) A method according to claim 26, wherein said one or more external authentication systems include:

a default web server authentication system;
an authentication plug-in; and
a third party authentication system.

28. (Original) A method according to claim 26, wherein:

said access system protects a plurality of resources, said plurality of resources includes said first resource, a second resource and a third resource;

said first resource uses said first authentication system for authentication services;
said second resource uses a second authentication system for authentication services, said second authentication system is separate from said access system; and

said third resource uses a third authentication system for authentication services, said third authentication system is separate from said access system.

29. (Original) A method according to claim 28, wherein:

said first authentication system is a default web server authentication system;
said second authentication system is a authentication plug-in; and
said third authentication system is a third party authentication system.

30. (Original) A method according to claim 26, wherein said step of relying includes:
accessing a pre-designated variable having a value; and
storing said value as an identification of an authenticated user.

31. (Original) A method according to claim 30, wherein said step of performing authorization services includes the steps of:

accessing one or more authorization rules for said first resource;
using said identification to access an identity profile; and
evaluating one or more attributes from said identity profile against said one or more authorization rules for said first resource to determine whether to authorize access to said first resource.

32. (Previously Presented) One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

acquiring user identification information from a first authentication system, said user identification information is associated with a request from a first user to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said first authentication system;

relying on said first authentication system for authenticating said first user;

using said user identification information to access an identity profile associated with said user identification information; and

performing, at said authorization system, authorization services for said request to access said first resource based on said identity profile associated with said user identification information;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

33. (Previously Presented) One or more processor readable storage devices according to claim 32, wherein relying on said first authentication system comprises the steps of:

receiving information about said request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.

34. (Original) One or more processor readable storage devices according to claim 32, wherein said method further comprises the steps of:

acquiring one or more data items in addition to said user identification information, said step of performing authorization services uses said one or more data items to attempt to authorize access to said first resource in response to said request.

35. (Original) One or more processor readable storage devices according to claim 32, wherein:

said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

36. (Original) One or more processor readable storage devices according to claim 32, wherein said method further comprises the steps of:

using said user identification information to create information for a cookie;
causing said cookie to be transmitted for storage on a client associated with said request; and

performing single sign-on services based on said cookie.

37. (Original) One or more processor readable storage devices according to claim 32, wherein said method further comprises the steps of:

using said user identification information to create information for a cookie;
causing said cookie to be transmitted for storage on a client associated with said request;

receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.

38. (Previously Presented) An access system, comprising:

a communication interface;
one or more storage devices; and

one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

acquiring user identification information from a first authentication system external to said access system, said user identification information is associated with a request from a first user to access a first resource,

relying on said first authentication system for authenticating said first user,
using said user identification information to access an identity profile associated
with said user identification information, and

performing authorization services for said request to access said first resource
based on said identity profile associated with said user identification information;

wherein said authorization services comprise determining whether said first user
is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first
user.

39. (Original) An access system according to claim 38, wherein:

said access system protects a plurality of resources, said access system provides
for use of one or more internal authentication systems and said access system provides for
reliance on one or more external authentication systems, said one or more external authentication
systems include said first authentication system.

40. (Original) An access system according to claim 38, wherein said method further
comprises the steps of:

using said user identification information to create information for a cookie;
causing said cookie to be transmitted for storage on a client associated with said
request;

receiving a request to access a second resource, said request to access said second
resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without
authenticating.

41. (Previously Presented) An access system according to claim 38, wherein-relying on said first authentication system comprises the steps of:

receiving information about said request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.

42. (Previously Presented) One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

acquiring a plurality of variables from a first authentication system, said step of acquiring is performed by an authorization system, said authorization system is separate from said first authentication system, said variables are associated with a first request from a first user to access a first resource;

relying on said first authentication system for authenticating said first user; and

performing, at said authorization system, authorization services for said request to access said first resource based on said plurality of variables;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

43. (Previously Presented) One or more processor readable storage devices according to claim 42, wherein relying on said first authentication system comprises the steps of:

receiving information from said first request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.

44. (Original) One or more processor readable storage devices according to claim 42, wherein:

said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

45. (Original) One or more processor readable storage devices according to claim 42, wherein said method further comprises the steps of:

using said plurality of variables to create information for a cookie;
causing said cookie to be transmitted for storage on a client associated with said request;

receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.

46. (Previously Presented) An access system, comprising:
a communication interface;
one or more storage devices; and
one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

acquiring a plurality of variables from a first authentication system external to said access system, said variables are associated with a first request from a first user to access a first resource,

relying on said first authentication system for authenticating said first user, and

performing authorization services for said request to access said first resource based on said plurality of variables;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

47. (Previously Presented) An access system according to claim 46, wherein-relying on said first authentication system comprises the steps of:

receiving information from said first request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.

48. (Original) An access system according to claim 46, wherein:

said access system protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

49. (Original) An access system according to claim 46, wherein said method further comprises the steps of:

using said plurality of variables to create information for a cookie;

causing said cookie to be transmitted for storage on a client associated with said request;

receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.

50. (Previously Presented) One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

acquiring user identification information from an authentication system, said user identification information is associated with a request from a first user to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said authentication system;

relying on said authentication system for authenticating said first user;

using said user identification information to create information for a cookie;

causing said cookie to be transmitted for storage on a client associated with said request to access said first resource; and

performing, at said authorization system, authorization services for said request to access said first resource;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

51. (Original) One or more processor readable storage devices according to claim 50, wherein:

said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

52. (Original) One or more processor readable storage devices according to claim 50, wherein said method further comprises the step of:

performing single sign-on services based on said cookie.

53. (Original) One or more processor readable storage devices according to claim 50, wherein said method further comprises the step of:

receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.

54. (Original) One or more processor readable storage devices according to claim 50, wherein said method further comprises the step of:

receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.

55. (Previously Presented) An access system, comprising:

a communication interface;

one or more storage devices; and

one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

acquiring user identification information from an authentication system separate from said access system, said user identification information is associated with a request from a first user to access a first resource,

relying on said authentication system for authenticating said first user,

using said user identification information to create information for a cookie,

causing said cookie to be transmitted for storage on a client associated with said request to access said first resource, and

performing authorization services for said request to access said first resource;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

56. (Original) An access system according to claim 55, wherein:

said access system protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

57. (Original) An access system according to claim 55, wherein said method further comprises the step of:

performing single sign-on services based on said cookie.

58. (Original) An access system according to claim 55, wherein said method further comprises the step of:

receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.

59. (Original) An access system according to claim 55, wherein said method further comprises the step of:

receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first

authentication system does include said first server and does not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.

60. (Previously Presented) One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving, at an access system, configuration information for a first resource, said access system provides for using one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said configuration information provides an indication to said access system to rely on a first external authentication system for said first resource;

receiving information for a first request from a first user for said first resource; relying on said first external authentication system for authenticating said first user; and

performing, at said authorization system, authorization services for said first request;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

61. (Original) One or more processor readable storage devices according to claim 60, wherein:

said access system protects a plurality of resources, said plurality of resources includes said first resource, a second resource and a third resource;

said first resource uses said first authentication system for authentication services;
 said second resource uses a second authentication system for authentication services, said second authentication system is separate from said access system;

 said third resource uses a third authentication system for authentication services, said third authentication system is separate from said access system;

 said first authentication system is a default web server authentication system;
 said second authentication system is a authentication plug-in; and
 said third authentication system is a third party authentication system.

62. (Original) One or more processor readable storage devices according to claim 60, wherein:

 said step of relying includes accessing a pre-designated variable having a value and storing said value as an identification of an authenticated user; and

 said step of performing authorization services includes the steps of:
 accessing one or more authorization rules for said first resource,
 using said identification to access an identity profile, and
 evaluating one or more attributes from said identity profile against said one or more authorization rules for said first resource to determine whether to authorize access to said first resource.

63. (Previously Presented) An access system, comprising:
 a communication interface;
 one or more storage devices; and
 one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

 providing for using one or more internal authentication systems,
 providing for reliance on one or more external authentication systems,

receiving configuration information for a first resource, said configuration information provides an indication to rely on a first external authentication system for a first resource,

receiving information for a first request from a first user for said first resource,

relying on said first external authentication system for authenticating said first user, and

performing authorization services for said first request;

wherein said authorization services comprise determining whether said first user is authorized to access said first resource; and

wherein authenticating said first user comprises verifying an identity of said first user.

64. (Original) An access system according to claim 63, wherein:

said access system protects a plurality of resources, said plurality of resources includes said first resource, a second resource and a third resource;

said first resource uses said first authentication system for authentication services;

said second resource uses a second authentication system for authentication services, said second authentication system is separate from said access system;

said third resource uses a third authentication system for authentication services, said third authentication system is separate from said access system;

said first authentication system is a default web server authentication system;

said second authentication system is a authentication plug-in; and

said third authentication system is a third party authentication system.

65. (Original) An access system according to claim 63, wherein:

said step of relying includes accessing a pre-designated variable having a value and storing said value as an identification of an authenticated user; and

said step of performing authorization services includes the steps of:

Application No. 09/886,515
Amendment dated April 13, 2006
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group 2136

PATENT

accessing one or more authorization rules for said first resource,
using said identification to access an identity profile, and evaluating one or
more attributes from said identity profile against said one or more authorization rules for said
first resource to determine whether to authorize access to said first resource.